CLAIMS

~~1. A method for system security in distributed systems, said method comprising the steps of:~~

~~a) making authentic statements by trusted intermediaries;~~

~~b) deriving freshness constraints from initial policy assumptions and the authentic statements; and~~

~~c) imposing freshness constraints employing authenticating principals to effect revocation.~~

~~2. A method according to claim 1, wherein said step b) comprises the substep I) of normalizing suffix constraints of the freshness constraint prior to applying other rules.~~

~~3. A method according to claim 2, wherein said substep I) comprises applying the following axiom,~~

~~$\vdash (A \,.\, B$ **notbefore** t_1 **notafter** $t_2) \supset (((t_1 \leq t_3) \wedge (t_4 \leq t_2)) \supset A \,.\, B$ **notbefore** t_3 **notafter** $t_4)$.~~

~~4. A method according to claim 1, wherein said step c) comprises specifying the time of revocation.~~

5. A method according to claim 4, wherein said step c) includes trusting principals not to lie when specifying the time of revocation certificates.

6. A method according to claim 5, wherein said step c) further comprises the substep I) of arbitrarily bounding certain revocation by adjusting the freshness constraints.

7. A method according to claim 6, wherein said substep I) comprises applying the following axioms,

$\vdash (A\ _{.}\ B$ **notbefore** t_1 **notafter** $t_2) \supset (((\text{A } \textbf{says} \text{ s } \textbf{at } t_3)\ (t_1 \le t_{now}, t_3 \le t_2)) \supset (\textbf{B says } s \textbf{ at } t_3))$; and

$\vdash (A$ **says** $(B\ _{.}\ A$ **notbefore** t_1 **notafter** $t_2)$ **at** $t_3) \supset (B\ _{.}\ A$ **notbefore** t_1 **notafter** $t_2)$.

8. A method for enforcing revocation in distributed systems, said method comprising the steps of:

a) issuing one or more initial assertions by one or more distinguished principals;

b) asserting, by the distinguished principals, one or more principals with authority for asserting a time stamped validity assertion pertaining to the validity of each initial assertion;

c) asserting the time stamped validity assertion to none or more initial assertions indicating their validity at the time of the time stamp;

d) asserting freshness constraints indicating a length of time and the initial assertions that the freshness constraints relate; and

f) verifying that a relation $| t_{now} - t_{time\ stamp} | \leq \delta$ is satisfied for each particular assertion necessary for verification of a secure channel, where $t_{time\ stamp}$ is a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification.

9. A method according to claim 8, wherein said steps a) and b) occurring concurrently.

10. A method according to claim 8, wherein in said step a) the distinguished principals are identification authorities.

11. A method according to claim 10, wherein said step a) includes issuing certificates, as initial assertions, by the identification authorities.

12. A method according to claim 8, wherein said step a) further includes asserting a validity of the initial assertion at the time of a time stamp employing a time stamp assertion.

13. A method according to claim 8, wherein said step d) includes asserting freshness constraints within said step b).

14. A method according to claim 8, wherein said step f) includes verifying the relation using a verifier which is a distinguished principal.

15. A method according to claim 8, wherein said step a) includes the substep of asserting, by the initial assertions, one or more relationships to one or more of the distinguished principals.

16. A method according to claim 15, wherein one or more of the relationships including asserting an employee relationship and asserting an identity of a person having the employee relationship.

17. A method according to claim 8, wherein said stop a) includes cryptographically certifying the initial assertions using a key of one or more of the distinguished principals.

18. A method according to claim 17, wherein in said step a) the distinguished principals are identification authorities.

19. A method according to claim 8, wherein said step a) includes storing the initial assertions in a trusted storage system, the trusted storage system being trusted by other principals as being an assertion by one or more of the distinguished principals.

20. A method according to claim 8, wherein said step c) includes storing the time stamped validity assertions in a trusted storage system, the trusted storage system being trusted by other principals as being an assertion of one or more of the distinguished principals.

21. A method according to claim 8, wherein said step c) includes issuing time stamped certificates by the one or more authorities for asserting the time stamped validity assertions.

22. A method according to claim 8, further comprising the step of:

g) distributing the time stamped certificates to storage systems and communication networks.

23. A method according to claim 22, wherein said step g) includes addressing the distribution of the time stamped certificates to one or more multicast addresses.

24. A method according to claim 22, wherein in said step t) distribution occurs at periodic intervals.

25. A method according to claim 8 wherein said step d) includes asserting the freshness constraints within the initial assertions.

26. A method according to claim 8, wherein said step d) includes asserting the freshness constraints by a risk taker.

27. A method according to claim 26, wherein the risk taker is a verifier.

28. A method according to claim 8, wherein in said step d) includes cryptographically certifying the freshness constraint and the initial assertions using a signing key.

29. A method according to claim 8, wherein said step d) comprises the substep of storing the freshness constraints and the initial assertions in trusted storage systems trusted by other entities as being an assertion of the principals making the assertion.

30. A method according to claim 8, wherein said step f) includes dynamically changing the time of verification.

31. A method for protecting an authority of one or more distinguished principals and enforcing revocation when the authority is compromised, said method comprising the steps of:

a) issuing one or more initial assertions delegating authority by a first one of the distinguished principals to a second one of the distinguished principals;

b) issuing one or more secondary assertions delegating authority by the second one of the distinguished principals to a third one of the distinguished principals;

c) repeating said step b) none or more times;

d) issuing one or more authoritative assertions by one or more of the distinguished principals;

e) asserting freshness constraints on assertions;

f) asserting a time stamped validity assertion to the assertions in said steps a)-e) indicating the validity of the assertions in said steps a)-e) at the time of the time stamp;

g) verifying that a relation $| t_{now} - t_{time\ stamp} | \leq \delta$ is satisfied for each particular assertion necessary for verification of a secure channel, where $t_{time\ stamp}$ being the time of a time stamp pertaining to the validity assertion of the particular assertion, δ being the minimum necessary freshness constraint pertaining to the particular assertion, and t_{now} being the time of verification.

32. A method according to claim 28, wherein said step d) further comprises including an assertion on behalf of a parent distinguished principal due to the delegated authority obtained by said steps a)-c), and wherein said step e) further comprises making a freshness constraint in assertions made by a child distinguished principal in said steps a)-d) more restrictive than freshness constraints made by the parent distinguished principal.

33. A method according to claim 31, wherein said steps a) and t) are performed concurrently.

34. A method according to claim 31, wherein said steps b) and f) are performed concurrently.

35. A method according to claim 31, wherein said steps d) and f) are performed concurrently.

36. A method according to claim 31, wherein inputs to the one or more principals is off--line.

37. A method for issuing certificates in a system for enforcing revocation in distributed systems, said method comprising the steps of:

a) designating a policy authority for dictating policy to subordinates;

b) asserting an organization subject to a policy of a policy authority;

c) issuing certificates for subordinate principals within the organization by the organization;

d) asserting, by the organization, a principal authorized as an authority for issuing time stamped certificates;

e) delegating authority for issuing time stamped certificates;

f) asserting freshness constraints on assertions; and

g) verifying that a relation $| t_{now} - t_{time\ stamp} | \leq \delta$ is satisfied for each particular assertion necessary for verification of a secure channel, where $t_{time\ stamp}$ being a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification.

38. A method according to claim 37, further including storing the assertions, time stamp and reference in a replicated directory having varying levels of persistent storage.

39. A method according to claim 38, wherein the replicating directory includes frequently replicating information in a high level directory, often replicating information in a medium level directory and infrequently replicating information in a low level directory.

40. A method according to claim 39, further including replicating time stamped assertions in the high level directory, replicating the time stamped assertions and delegation assertions in the medium level directory, and replicating the time stamped assertions, the delegation assertions and identification assertions in the low level directory.

41. A method according to claim 38, further including storing each assertion in a trusted storage system being trusted by other principals as being an assertion by one or more distinguished principals.

42. A method according to claim 38, further including cryptographically certifying the assertion using a key of one or more of the distinguished principals.

43. A method for system security in a distributed system network, comprising the steps of:

a) receiving a policy in the distributed system network;

b) preparing an initial statement in the distributed system network in response to said policy;

c) preparing a second statement of an assigned revocation authority in the distributed system network in response to said policy, said second statement being associated with said initial statement;

d) preparing a third statement of a freshness constraint period in the distributed system network in response to said policy, said third statement being associated with said initial statement;

e) preparing a validity statement at said assigned revocation authority in the distributed system network in response to said policy, said validity statement including a verification status at some temporal reference;

f) providing said initial statement, said second statement, said third statement, and said validity statement to a verification authority in the distributed system network; and

g) selectively verifying said initial statement at said verification authority in response to said initial statement, said second statement, said third statement, and said validity statement.

44. A method according to claim 43, wherein any of the initial statement, said second and third statements, and said validity statement has an "expiration date" and/or "not valid before" date.

45. A method according to claim 43, wherein any combination of said initial statement, said second statement, and said third statement occurs concurrently.

46. A method according to claim 43, wherein the assigned revocation authority is an entity making the initial statement in step b).

47. A method for system security in a distributed system network, comprising the steps of:

a) receiving a first term policy in the distributed system network;

b) preparing an initial statement in the distributed system network in response to said first term policy;

c) preparing a second statement of an assigned revocation authority pointer in the distributed system network in response to said first term policy, said second statement being associated with said initial statement;

d) preparing a third statement delegating a freshness constraint period to said assigned revocation authority pointer in the distributed system network in response to said first term policy;

e) providing a medium term policy to said revocation authority pointer in the distributed system network;

f) preparing a fourth statement of medium term delegation at said revocation authority pointer in response to said medium term policy, said medium term delegation naming an assigned revocation authority;

g) preparing a fifth statement of a particular freshness constraint period at said revocation authority pointer in response to said medium term policy;

h) providing a third term policy to said revocation authority in the distributed system network;

I) preparing a validity statement at said assigned revocation authority in the distributed system network in response to said third term policy, said validity statement including a verification status at some temporal reference;

j) providing said initial statement, said second, third, fourth, and fifth statements, and said validity statement to a verification authority in the distributed system network; and

k) selectively verifying said initial statement at said verification authority in response to said initial statement, said second, third, fourth, and fifth statements, and said validity statement.

48. A method according to claim 47, wherein any of the initial statement, said second, third, fourth, and fifth statements, and said validity statement has an "expiration date" and/or "not valid before" date.

49. A method according to claim 47, wherein any combination of said initial statement, said second statement, and said third statement occurs concurrently.

Attorney Docket No. Stubblebine 1

50. A method according to claim 47, wherein said fourth statement and said fifth statement occur concurrently.

51. A method according ~~to claim~~ 47, wherein the assigned revocation authority pointer is an entity making the initial statement in step b).

Add B1